United States Department of State

Privacy Impact Assessment (PIA)

Consular Affairs Enterprise Service Bus

(CAESB) 01.00.00

Last Updated: May 1, 2015

Bureau of
Administration

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

a. Date PIA was completed: May 1, 2015

b. Name of system: Consular Affairs Enterprise Service Bus

c. System acronym: CAESB

d. IT Asset Baseline (ITAB) number: # 6187

e. System description (Briefly describe scope, purpose, and major functions):
The scope of the Consular Affairs Enterprise Service Bus (CAESB) is to provide reusable enterprise level services such as name and biometrics checks in support of passport and visa application processing. CAESB moves, reformats and transforms data between Department of State systems and external interfaces. In addition, the purpose of CAESB is to provide a common structure and method of governance for service offerings as the Department of State moves toward implementation of Service Oriented Architecture (SOA).

f. Reason for performing PIA:

- ☒ New system
- ☐ Significant modification to an existing system
- ☐ To update existing PIA for a triennial security reauthorization

g. Explanation of modification (if applicable): N/A

h. Date of previous PIA (if applicable): N/A

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

CAESB processes personally identifiable information (PII) elements when Department of State employees use Consular Consolidated Database (CCD) applications that may request access to the CAESB system for executing queries and other transactions. The following PII elements are collected: names of individuals, birthdates of individuals, SSN or other identifying numbers including, individual ID numbers from other sources, addresses, phone numbers, email address of individuals, images/biometric ID, and personal financial information such as bank account numbers.

PII that is processed by CAESB is not permanently retained. Some PII data may be stored temporarily in system logs or the audit logs. Log information is retained online for a period of three days before it is archived offline or purged.

b. How is the information collected?

CAESB system does not collect any PII data. All PII processed by CAESB is obtained from the following Department of State systems:

- Consular Consolidated Database (CCD)
- Front End Processor (FEP)
- Consular Lookout and Support System (CLASS)
- Non-Immigrant Visa (NIV)
- Immigrant Visa Overseas (IVO)
- Independent Namecheck (INK)
- Travel Document Issuance System (TDIS)
- Passport Records Imaging System Management (PRISM)
- Consular Electronic Application Center (CEAC)

c. Why is the information collected and maintained?

All PII processed by CAESB is obtained from and maintained by other State Department systems (See section 3.b). Each element of PII processed by CAESB is necessary for the adjudication of passport and visa applications. The PII elements are required to determine passport and visa eligibility, issue the passport and visa documents, and to contact applicants.

d. How will the information be checked for accuracy?

All PII processed by CAESB is obtained from and maintained by other State Department systems (See section 3.b). CAESB is totally dependent upon the validity, safeguards, and accuracy of the PII security controls of data system sources, which can be found in the PIAs for those systems.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The following authorities provide for the administration of the program supported by CAESB:

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 8 U.S.C. 1101-1503 (Immigration and Nationality Act of 1952, as amended).
- The Immigration and Nationality (INA) act, 8 U.S.C. 1202, Section 222 (f) (Confidentiality of Visa records)
- 8 U.S.C. 1401-1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541-1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2651a, 2705 (2007); (Executive Order 11295, August 5, 1966); 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Control of Citizens)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- Section 236 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001
- 22 C.F.R. parts 50 and 51, Citizenship and Naturalization and Passports and Visas
- Immigration Act of 1990
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA96) (P. L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P. L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000)
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)
- Child Status Protection Act of 2002 (HR 1209) (P. L. 107-56)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The primary risk is misuse of the system by an authorized CAESB System Administrator tampering with the system to extract PII from the CAESB transaction stream. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

These risk factors are mitigated through the use of technical, management, and operational security controls in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). CAESB application data

is protected by multi-level system security. The defense-in-depth system security includes State Department intranet security, CAESB application security, Department of State site physical security and management security. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports. In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application.

4. Uses of the Information

a. Describe all uses of the information.

The CAESB system is a component that provides reformatting and data transformation capability to various front-end client applications for executing queries and other transactions with back-end systems and/or databases. It serves as a controller/translator where data requests from one application (client) are redistributed to various application systems (clients/servers). It consists of an engine that matches data front-end queries to the back-end databases. Some PII may be retained temporarily online in transaction logs for a period of three days. After that, the logs are permanently archived off-line by State Department Enterprise Operations. PII is retained for reference during investigations involving a breach of security or misuse of government systems.

b. What types of methods are used to analyze the data? What new information may be produced?

CAESB does not create or modify any PII content in processed transactions nor does it perform any content analysis of the PII.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

CAESB does not use any commercial information or public information. CAESB obtains PII from other Federal agencies including the U.S. Department of Justice and the Social Security Administration for visa and passport document adjudication purposes and transmits it to other Department of State systems. No PII resides within the CAESB system.

d. Are contractors involved in the uses of the PII?

Contractors are involved with the design, development, and maintenance of the system. Privacy Act information clauses have been inserted into all statement of

work and become part of the signed contract. Each contractor employee is required to attend mandatory briefings that cover the handling of PII information prior to working on the task. Contractors and government employees are also bound by the same security rules and standard operating procedures.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.
Contractors involved in the design, development, and maintenance of CAESB are required to have a moderate risk public trust access authorization. This includes a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of CAESB hardware or software must have at least a secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by the Bureau of Diplomatic Security (DS).

5. Retention

a. How long is information retained?
The PII is maintained online in transaction logs for a period of three days. After that, the logs are permanently archived off-line by State Department Enterprise Operations.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.
Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater the risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of information aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of CAESB throughout the lifetime of the data. Accuracy of the data is dependent on the individuals providing accurate self-identifying information. The information is only retained in online logs for three days. Additionally, these logs are never accessed again in the course of normal operations so they introduce negligible additional risk to the system.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

CAESB transfers PII internally between the State Department systems listed in section 3.b. The information is transferred to support the operations of each system. CAESB only shares audit trail information with authorized CAESB System Administrators within Diplomatic Security. No other bureaus, offices or organizations receive information from CAESB. The shared information is for fraud assessment purposes, and may include a review of all elements of PII for any transaction being reviewed.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

CAESB transmits all data over the secure State Department intranet which is safeguarded by State enterprise-wide security controls.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The primary risk is misuse of the system by an authorized CAESB System Administrator tampering with the system to extract PII from the CAESB transaction stream. Intentional and unintentional disclosure of PII by personnel can result from social engineering, phishing, abuse of elevated privileges or a general lack of training. Misuse may result in blackmail, identity theft or assumption, account takeover, physical harm, discrimination, or emotional distress to individuals whose PII is compromised and administrative burdens, financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.

These risk factors are mitigated through the use of technical, management, and operational security controls in accordance with the Federal Information Security Management Act (FISMA) of 2002 and information assurance standards published by the National Institute of Standards and Technology (NIST). CAESB application data is protected by multi-level system security. The defense-in-depth system security includes State Department intranet security, CAESB application security, Department of State site physical security and management security. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g. firewalls, intrusion detection systems, antivirus software), and audit reports. In addition, these controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for the Department of State. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?
CAESB shares Passport and Visa applicant's financial information with the Pay.gov website in order to process payments. Payment information is shared with the website so Passport and Visa applicants can pay fees through Department of State applications.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?
Information is shared outside of the Department through encrypted connections. Safeguards to protect this information include firewalls and encryption that follow Department of State guidelines.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.
CAESB data risk is mitigated by securing firewalls to limited access only and encryption of the data.

8. Notice

The system:

☒ contains information covered by the Privacy Act.
Provide number and name of each applicable systems of records.
Passport Records – STATE-26

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?
CAESB only processes transactions containing PII data that is collected by other CA systems. CAESB does not collect PII data directly from any users. Notice is provided to the individual at the initial point of collection.

b. Do individuals have the opportunity and/or right to decline to provide information?
CAESB does not collect PII data directly from any users. See 8a.

c. Do individuals have the right to consent to limited, special, and/or specific use of the information? If so, how does the individual exercise the right?
CAESB does not collect PII data directly from any users. See 8a.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.
CAESB does not collect PII data directly from any users. See 8a.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?
There are no procedures for an individual to gain access and amend information in CAESB. CAESB only processes transactions containing PII data that is collected by other CA systems. The systems sourcing the data to CAESB have the responsibility for meeting this requirement, information about which can be found in their respective PIAs.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.
The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?
Access to the CAESB component is restricted to cleared, authorized Department of State CAESB System Administrators via the Department's unclassified intranet. To access the system, administrators must be an authorized user of the Department of State's unclassified network. Each authorized administrator must sign a user access agreement before being given an account with CAESB administrator privileges. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. System administrators can access the CAESB component only at the central server location to perform component maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entity is strictly prohibited.

Personnel accessing CAESB information must be authorized by CA/CST management. Authorized personnel require a user ID and password to access CAESB information. User access to CAESB information is restricted to administrator roles only.

Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.)

b. What privacy orientation or training for the system is provided authorized users?

All CAESB administrators must attend a security briefing and pass the computer security and privacy awareness training prior to receiving access to the system. In order to retain the access, users must complete annual refresher training.

Administrators must read and accept the Computer Fraud and Abuse Act Notice and the Privacy Act Notice that describe the expected use of these systems and how they are subject to monitoring prior to being granted access.

All contractors involved with the design, development, and maintenance have Privacy Act contract clauses in their contracts and all other regulatory measures have been addressed. They are informed of the established rules of conduct and undergo training on handling information under the Privacy Act of 1974, as amended.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, restrict access to system administrators and are regularly reviewed, and inactive accounts are promptly terminated. Also, as mentioned earlier, the system audit trails that are automatically generated are regularly reviewed and analyzed. As a result of these actions, the residual risk is moderate.

11. Technologies

a. What technologies are used in the system that involves privacy risk?

CAESB does not use any technology known to introduce additional privacy risk.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Since CAESB does not use any technology known to elevate privacy risk, the current system safeguards in place are satisfactory. Routine monitoring, testing, and evaluation of security controls are conducted to ensure that the safeguards continue to fully function.

12. Security

a. What is the security certification and accreditation (C&A) status of the system?
The Department of State will operate CAESB in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department conducts risk assessments to identify appropriate security controls to mitigate risk, implement those controls, and perform audits on a regular basis to ensure that the controls continue to work effectively. In accordance with the Federal Information Security Management Act (FISMA) of 2002 provision for the certification of this system, CAESB received its Authorization To Operate in November 2014. This document was updated as part of the triennial reauthorization of the system.